Ethical and responsible IoT

EJLT European Journal of Law and Technology

Ethical and Responsible IoT: The Edinburgh Initiative

Andrés Domínguez, Ewan Klein, Charles Raab and James Stewart*

Abstract

We describe the work of an Action Group on Governance and Ethics in assessing the use of a new Internet of Things (IoT) infrastructure in the University of Edinburgh. We review three use cases of IoT at the University in the context of a framework for ethical and responsible IoT that could be generalised to the University's wider programme of data-driven innovation and to universities and research centres. We also explore a broader set of issues in ethical practice that reach beyond the boundaries of IoT in research and education.

Keywords: internet of things, ethics, responsible innovation, accountability

1 Introduction

The Internet of Things (IoT) comprises a cluster of technologies and business models spanning sensors and actuators, hardware devices, networking, data processing and data-intensive services. It is a rapidly growing area that underpins many new forms of relationship between people, organisations and computing services and has the potential for significant scientific, social and commercial impact. Pundits continue to predict massive levels of growth in investment and deployment of IoT systems. In this article we explore how a university attempting to develop research infrastructure to support IoT research and

* School of Social and Political Science, University of Edinburgh (Domínguez, Raab, Stewart) and School of Informatics, University of Edinburgh (Klein).

commercialisation is dealing with the imagined and real ethical, innovation, and reputational issues this implies.

IoT involves connecting 'things' to online services and to each other via internet protocols, posing significant social, legal and ethical challenges that require new ways of thinking and regulating. Use cases can be found in industrial sites, dense urban spaces and rural areas. These include real-time integration of supply chains; new types of non-computer interfaces to online services using voice and face recognition; networks of low-cost sensors in urban spaces to gather data to inform or automate planning, traffic management, pollution control and scientific research; and agriculture management by means of monitoring systems and smart control of inputs. The label 'IoT' covers a range of concepts from R&D and commercial sectors, including 'ubiquitous computing', embedded systems, smart homes and cities, and industry 4.0. A representative example is tracking indoor space occupancy, yielding management data for promoting the efficient use of spaces and energy as well as the convenience of those using monitored places. One of the use cases discussed here illustrates this example; it brings to light likely tensions between purposes as well as the implications of monitoring for privacy protection, freedoms and rights. Mitigating adverse impacts requires the application of ethical principles and procedures as well as legal rules. In a later section of this article, we examine the shaping of these measures.

The stated goal of the University of Edinburgh's IoT Initiative is to develop and maintain world-class IoT infrastructure and research capabilities that will attract students, academic collaborators and industrial partners from around the world.[1] At the outset (in early-2016), the Initiative was led by an informal co-ordinating group reflecting a diversity of actors: operations staff from Information Services, academic staff, a representative of the City Council and the President of the University's Student Association. The overall goal of the co-ordinating group was to ensure a coherent and 'joined up' approach within the University and with external bodies by developing an overall vision, defining objectives, monitoring progress, sharing knowledge, and providing oversight.

[1] See http://iot.ed.ac.uk/iot-initiative/

The IoT Initiative can be seen as a testbed for achieving many important goals for a range of data technologies and for devising governance. To do this, four specialised 'action groups' were established, covering governance and ethics (with an emphasis on policy aspects); security and privacy (focusing on technical aspects of IoT); marketing and engagement; and teaching and learning. The initial remit of the Governance and Ethics Action Group[2] (hereinafter 'the AG') was to develop policies, principles and procedures to ensure high standards for the ethical and privacy-preserving handling of data. The intention was to ensure that projects developed within the Initiative comply with current data protection legislation to protect the information privacy of humans whose personal data might be processed and to avoid institutional reputational damage from any ethical and legal deficiency. Beyond privacy and data protection, a further aim was to establish a broader scheme for setting high ethical standards and responsibility via appropriate accountability procedures.

The AG's work was commissioned while the design and deployment of the new infrastructure were still at an early stage: this brought advantages and challenges. It meant that pilot projects could be assessed against ethical guidelines, could be accountable, and could act as exemplars for future projects. However, as such guidelines were still to be written, tested and put in place while the first projects developed, the AG adopted a 'learning by doing' strategy. It also required that the AG inform itself about the existing procedures and machinery for ethical review of research proposals across the landscape of a large, research-intensive university. It was anticipated that IoT research would be likely to embrace many academic disciplines, departments, and external organisations, and to generate novel kinds of project proposal that the existing research approval structures were not necessarily equipped to scrutinise and evaluate. Given the University's commitment to base all forms of data-driven innovation and research on a solid foundation of ethics, legal compliance and public trust,[3] gathering such knowledge and basing principles and proposals on it for the purposes of IoT also gained relevance to the

[2] Three of the authors constituted the core of the AG and the other was closely involved.
[3] See, for example, https://ddi.ac.uk/about-us-data-innovation/ethics-governance/.

University's central planning and implementation of its wider data-driven innovation programme.

This article reflects on the work of the AG during the first two years of the Initiative's operation.[4] We offer an account of how ethical principles and procedures were devised and put into action with three IoT pilot projects. We discuss the challenges encountered in embracing both project delivery and ethical concerns across different scenarios of infrastructure usage. The next section outlines the technical and organisational architectures of the Initiative, followed by a broad sketch of ethical considerations and questions that pertain to innovation programmes exemplified by the Initiative. We then describe the pilot projects and specific learning points, before discussing general ethical and governance issues.

2 Technology and data ethics

A preoccupation with the ethics of technology has a long history, covering diverse fields and driven by a range of critical agendas, from workers' rights to feminist perspectives. This has been especially so when the adoption and use of technology may cause harm or consolidate existing socio-economic inequalities, or provoke major social or environmental change (Bauer, 1995; Wajcman, 2010). Contemporary 'data ethics' has close ties to established concerns for the ethics and governance of information and communications technologies (ICT), which can be traced back to Wiener's (1954) work on the foundations of cybernetics. Moor (1985) later proposed 'Computer Ethics' as a field in its own right on the grounds that, unlike other technologies, computers were versatile and 'logically malleable'. Data ethics has become an established field of research and practice in an age of intensive and extensive surveillance. This field has been given considerable new impetus by the rise of social media, mobile devices, IoT, machine learning and artificial intelligence (AI), especially when they enter the realms of the home, health or security.

[4] The AG is in abeyance as a group as a result of internal reorganisation of functions within the University.

However useful as a starting point, the problem with technology-push approaches to ethics is the assumption that professionals create new products and services in an orderly fashion. Studies of technology-based innovation show that this is rarely the case (MacKenzie and Wajcman, 1985; Williams et al., 2005), as new technical services and products are generally modified, reconfigured, customised and used in unexpected ways responding to context-dependent contingencies (Stewart and Williams, 2005). ICT allow *ad hoc* configuration of standardised components by agents and organisations that might not have the insight, skills or governance to follow advanced ethical practice and may be developed in local culture and contexts where specific ethical issues are not salient or are deliberately suppressed. Such an understanding of innovation further complicates the elaboration of ethics in technology and the identification of nexuses of responsibility. The concept of 'responsibility' is invoked in the ethics debate, often being conflated with notions of accountability and liability (Hijmans and Raab, 2018; Raab, 2017). The General Data Protection Regulation (GDPR, 2016), for example, includes accountability as a principle,[5] making explicit reference to the *responsibility* of data controllers. It is often suggested that implementing accountability mechanisms can help to build trust (ICO, 2019). Trust, trustworthiness and accountability are important related concepts for the Initiative and are discussed in section 5.

Many everyday services rely on automated, behind-the-scenes data collection and processing from a mix of connected devices and online sources, with no human intervention. Regulating the use of IoT infrastructure and applications and ensuring accountability for the design of underlying data-management processes associated with other 'smart' developments is difficult in that these innovations are explicitly predicated on the convenience of 'hiding' the operation of computers in everyday situations (see e.g. Weiser, 1999). Moreover, since many IoT deployments consist of systems-of-systems, accountability, governance and responsibility may be distributed across numerous people and organisations (Singh et al., 2018). Accountability and ethical concerns extend beyond

[5] Article 5(2) of the GDPR reads: 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]'

individuals and data controllers when developers delegate decision-making to algorithms (Martin, 2018; Mittelstadt et al., 2016; Singh et al., 2018).

Many contemporary uses and visions of IoT have been explored under the banner of 'surveillance studies', which critically engages with the political drivers and consequences of sets of practices using technological instruments where these pose issues of ethics, legality, and human rights. Marx (1998; see also Raab, 2012) sketched an ethics for the 'new surveillance', perceiving that established means of regulation, largely through law, was losing potency in the face of the development and ubiquitous deployment of ICT. The ethical turn, itself, is controversial, with some viewing it as a (deliberately) less rigorous approach that lacks the strength of law, while technological design solutions to human rights problems are sometimes regarded sceptically as antagonistic to legal regulation (van Dijk et al., 2018). How new forms of regulation should relate to the law and rules, and where they should be located in a multi-layered landscape stretching from the individual to the global, are much debated. So, too, is the role of, and relationships between, principles, norms, guidelines and other forms of 'soft law' governing emerging technologies (Baldini et al., 2015).

Issues of aggravated social exclusion and 'data divides' are also pressing. Specific populations may (intentionally or not) be excluded from the purported benefits of IoT— or exposed to certain harms —owing to algorithmic biases, geographical constraints or lack of representation. Furthermore, the growing invisibility of IoT devices and the opacity of the data flows they enable problematises the conventional definition of the informed end-user and brings about the emergence of unaware subjects (Crabtree et al., 2018; Urquhart et al., 2018). Any ethical guidelines for researchers and developers should address the privacy, autonomy and interests of incidental and intended users alike, as well as of potential future ones who might be affected. While academic institutions focus on ethics risks arising from research, technology developers are perhaps under more pressure to consider potential future harms of their creations, thus entering into the domain of risk analysis and engaging in debates between precaution and pressing forward with innovation to realise the potential value of new knowledge and things.

These issues are applicable to IoT insofar as IoT facilitates applications that are ostensibly 'beneficial' but that nonetheless may harm individual rights and freedoms as well as a range of collective interests and social or political values (Jameson et al., 2019; Wright and Raab, 2014). Some ethical precepts are highly abstract but — if appropriately translated into procedures, guidelines, training, reflection and support that can be used 'on the ground' — seem nevertheless useful in addressing not only IoT's intended purposes and stakeholders, but its externalities as well. Applying ethics to IoT is thus a question of augmenting the application of legal requirements for, for example, accountability and transparency by means of other instruments that may be more adaptable to rapidly changing technologies and to the implications of economic, managerial, and public-service interests that rely upon surveillance systems often found in data-oriented innovations. Ethical principles concerning the treatment of humans by humans regardless of different social roles and statuses, and concerning the relationship between 'government' and 'the governed' in a variety of institutions including the state, also underpin transparency and accountability as necessary values in IoT and other ICT systems. Hence our preference for 'ethical and responsible IoT' as a fuller expression of what is required.

Of course, ethical principles need to be grounded in procedures and practices of 'doing ethics'. For example, universities have well-developed practices related to the ethics of research, in terms of training, principles and procedures. These are often very discipline-specific, ranging from lightweight tick-box exercises to rigorous regulation in fields such as biomedicine. Alongside this, professional codes of conduct govern psychologists, anthropologists, engineers, physicians, librarians, and many others. The more general 'turn to ethics', remarked on above, has led to an abundance of principles, procedures, training, 'toolkits', advisory boards and the like to support previously ethics-light domains. These come in many forms, including guidelines framed by philosophers, grounded in 'Ethics', which provide crash courses in philosophical principles as their starting point (see e.g. Santa Clara University, 2015); tools produced for using participatory design techniques for inclusive and ethical systems development (Urquhart, 2017); frameworks from the social sciences for 'engaging the public'; policy-driven frameworks and programmes of training such as Responsible Research and Innovation (see e.g. ORBIT-RRI, 2018); and many reviews

and analyses by newly founded ethics institutes and centres, public, private and academic. This flurry of activity illustrates the desire, not least on the part of action-oriented academics, that a consideration of ethics should be routinely integrated into technology and service development alongside business models and human interface design. We return to this discussion in section **7**.

3 Brief Overview of the Edinburgh IoT Initiative

To date, the University of Edinburgh IoT Initiative has established an experimental wide-area communications network across the city and surrounding districts using LoRaWAN, a long-range, low-power radio protocol[6] that is becoming widely adopted across the world for both public and private networks (LoRa Alliance, 2019). At the time of writing, the University's LoRaWAN network comprised nine gateways with coverage across most of the city. Above this physical communications layer, data captured by IoT devices is passed to a centralised software system for data storage, visualisation and analysis. The resulting framework for end-to-end processing of data is made available 'as a service' to University staff, students, and external partners. The infrastructure has been designed to be as open as possible, in the sense that every hardware and software component should ideally be accessible, modifiable and available for experimentation within the constraints of security concerns. This is to encourage innovative research and development across a wide range of IoT components, including physical devices, network configuration, middleware, applications, and services.

The University's IoT service is designed to be an enabling resource for research in fields as diverse as agriculture; environmental monitoring such as air quality, biodiversity, and flooding; energy use; urban planning; and monitoring of individuals' health. The infrastructure, however, is not only aimed at research; it can also be used by the operational side of the University (e.g., Estates, Libraries, and others), for administrative purposes such as tracking the location and usage of assets, monitoring space usage and

[6] The LoRaWAN specification was developed in 2015 by the LoRa Alliance, a consortium of technology companies including Semtech, Cisco, IBM, among others (https://lora-alliance.org/).

assessing environmental conditions within buildings. Given the geography of the University's central campus within Edinburgh, it would be difficult, if not impossible, to circumscribe the activities falling within the range of the IoT infrastructure as purely those belonging to the University and indeed much of the expected value of the Initiative is its potential to provide real-time data about the city as a whole.

Applications using the infrastructure may collect data — whether intentionally or incidentally — that reflects the activities of people as they occupy and move through city spaces and buildings, conduct their social relationships, and interact with connected devices. Key concerns, therefore, are whether individuals and organisations have been made sufficiently aware of the aims and governance mechanisms of the IoT Initiative and how far they are able to assert their interests and rights, including information rights, in relation to the Initiative and to projects using its services. These concerns provided the rationale for establishing the AG as a governance structure tasked with protecting privacy, ensuring the ethical collection and use of data, reviewing potential benefits and harms ensuing from proposed IoT projects, making explicit to service users the steps they are expected to take for building and maintaining trust in the University, and providing the large diversity of likely users with the tools and information necessary to do this. The next section shows how ethical and data protection issues have surfaced and been addressed in the course of three pilot projects undertaken within the Initiative's auspices. The projects described represent a range of generic IoT use cases and thus provide useful transferable experience.

4 Use Cases

4.1 Office Environment and Occupancy Monitoring

In 2016–17, the University rehoused several hundred staff from an operational services department, previously scattered across many sites, in a large, multi-storey open-plan office building with bookable glass-walled meeting rooms.[7] Staff had to adjust to working in this highly co-visible environment. A pilot project to collect information about meeting-

[7] This case study is drawn from Magill et al. (2018).

room occupancy and environmental conditions in the office spaces was seen as providing a useful test of the emerging IoT infrastructure while also collecting operationally valuable data. The information gathered by the project was intended to help address two questions of concern to building managers: (i) was the configuration of meeting spaces appropriate for the needs of occupants?; and (ii) were the environmental conditions, particularly in terms of heating and ventilation, satisfactory in the open-plan offices?

The project deployed many devices linked with Bluetooth and LoRaWAN protocols. First, Estimote[8] Bluetooth beacons with auxiliary sensors were attached to chairs in a small meeting room. An additional device containing an accelerometer and light-level sensor was placed on the door, capturing door movement as well as showing whether the light was on. Second, sensors for light level, temperature, atmospheric pressure and relative humidity were placed near desks across one wing of the open-plan area.

The project was carried out before the AG was fully established. Nevertheless, before installing the sensors, the project manager carried out a Privacy Impact Assessment (PIA)[9] that was careful to document that no personal data would be captured by the sensors. Information about the project was communicated in two ways: (i) by sending an initial email announcement to all building users; and (ii) by attaching an explanatory notice to the wall of the monitored meeting room.

As a complement to the more technical and data-centric aspects of the project, two members of the project team undertook to ask more qualitative questions about the experience and reactions of the staff who had interacted with the monitoring devices (Magill et al., 2018). This was motivated in part by the understanding that it was important to anticipate possible adverse reactions from diverse people and to design this and future projects to obviate or minimise those concerns. The information was collected from building occupants through a combination of focus groups and semi-structured interviews.

---

[8] These are small, low-power devices that can be used to measure indoors location. See https://estimote.com for more details.

[9] Under the GDPR, the function of a PIA has largely been replaced by a Data Protection Impact Assessment (DPIA).

Two results are striking. First was the extent to which participants felt underinformed about the nature and goals of the project. Although the initial communication measures that were adopted (email, information poster) 'ticked the box' in terms of standard approaches to data protection compliance, they fell far short of engaging people's attention and interest. As a result, the affected people were unable properly to understand the what, how, and why of data collection via IoT devices.

Second, while privacy was not originally a primary concern of the qualitative study, reflections on privacy and surveillance surfaced frequently in the comments of the study participants. The physical boundaries of the spaces in question were clearly important in determining what were perceived to be 'information-spaces' (Jiang and Landay, 2002). The project chose to monitor a meeting room because it was a common space, not linked to any specific individuals and therefore considered less likely to trigger privacy concerns. By contrast, the desks that people occupied in the open-plan offices defined much more personal information spaces, albeit not demarcated by clear-cut physical boundaries. It was evident that many participants saw the monitoring of their desks as a source of concern and were worried about its potential to act as a 'foot in the door' that would expand and extend monitoring activities across the University estate.

A final point to note is that many of the study participants felt that the occupancy monitoring could have been carried out in a more inclusive and participatory manner in which the issues that most affected the performance, comfort, health and well-being of employees within the building would have been placed centre-stage, rather than being secondary to the goals of maximising managerial efficiency.

4.2 Library and study space occupancy monitoring

Space utilisation is identified as an important area for developing strategies within the 'intelligent campus' approach described by the UK's JISC (formerly the Joint Information Systems Committee), and the problem of insufficient workstations and learning spaces looms large (JISC, 2018; see also Clay, 2017). Although we will not address the issue here, the Covid-19 pandemic has further intensified the challenges of space utilisation in universities.

In response to a perception by Edinburgh students that there was insufficient study space across the University's campuses, the Student Association and the Library and Information Services division met with the core IoT development team to explore options for expanding an 'under-desk' anonymous occupancy system in a large study space covering the whole of the University's Main Library, and subsequently other study spaces. Apart from addressing the needs of students and other Library space-users, the service would also help senior Library management staff to acquire more accurate information about usage of the different forms of study space on offer, as evidence for future provision in library-based study/learning facilities and financial negotiations with other University divisions. With 2,000+ study desks spread throughout the eight storeys of the Main Library, students struggled to identify areas where they stood a good chance of finding an unoccupied desk. This led to complaints via the Student Association as well as negative, much-publicised, and embarrassing reports in National Student Satisfaction Surveys.

Before the AG's involvement, an initial pilot attempted to adopt the same sensing devices as those used in the office occupancy-monitoring project (section 4.1). These were installed on chairs and walls within one of the Main Library study areas. However, within a short space of time, most of the devices were stolen or vandalised and the pilot was consequently abandoned. As an alternative, it was decided to use data collected at the Library entrance gates, which are accessed via the University ID card. A recent requirement for Library users also to 'swipe out' when leaving the building meant that this data could be used to assess the number of people in the Library minute by minute. Data from the gates was encrypted and matched with basic data on the individuals (their School and College within the University and their course of study) and then further anonymised and aggregated before being made available to management and as real-time information for Library users. A 'traffic light'-style system was introduced on the Library web page and on a screen in the entrance hall to help students decide if it was worthwhile looking for a study space in the building. The AG was involved in scrutinising the Library's PIA for this phase of the project; the PIA was amended in accordance with the AG's recommendations.

However, at peak times it remained hard to find a seat, partly due to a culture of 'desk blocking' by Library users, so an additional method was sought that might help identify

available areas. Possible solutions using under-desk monitors, CCTV with image recognition or infra-red cameras were discarded as too expensive or potentially more intrusive. Therefore, the Library proposed to repurpose existing real-time logs of device connections (i.e., from smartphones, tablets or laptop computers) to the University Wi-Fi network. The working hypotheses were that this method would allow anonymised measurement, as no personal data would appear in any of the databases or reports. Since this method would not require new infrastructure, it was then proposed by a senior University manager that the information could be collected for *all* the centrally managed study spaces across the University. The main purposes would be: (i) to show students alternative study places that are currently 'under-used', perhaps with maps indicating how to reach them; and (ii) to allow planning of facilities in those other spaces. It would also help in negotiations to create new spaces.

The AG was consulted on the new PIA that was carried out for this proposed system and a range of practical and ethical concerns were addressed. The AG recommended consultation with students and academic staff about the implications of the system's deployment, both in the planned form, and in future extensions. However, the AG rejected an initial proposal to conduct a questionnaire survey, because the proposed system of data collection and reuse, and potential issues it raised, were more complex than could be communicated in a simple information sheet and a short set of questions. As an alternative, the AG designed and implemented a programme of focus groups based on a number of scenarios with a co-design element (e.g., Hyysalo and Hyysalo, 2018; Steen, 2011), engaging with students and academic staff across the University.[10] The AG wished to use this case to explore the issues and to understand how to involve the broader University community in debating and setting the agenda for IoT in the context of existing practices, policies and institutional strategy.

The use case was also discussed in detail in a range of forums: most notably, a half-day workshop with University ethics research committee officers and a research seminar with

[10] The authors are grateful for the assistance given by Yazmin Morlet Corti and Benedetta Catanzarati in devising and conducting these focus groups.

staff and students, in which two hour-long group-work sessions investigated the practical and ethical issues of how to design and govern this project, as well as the more general case of indoor monitoring in organisations. The AG further proposed that the introduction of occupancy monitoring should not be seen merely as the deployment of an information service, but as a tripartite period of research, pilot implementation, and evaluation; and that clear parameters should be defined for the degree of consultation that any future extension would require.

These discussions raised specific issues that needed to be addressed:

- Encouraging more active forms of engaging with Library users over potentially controversial services, in place of the rather passive current approach (e.g., signage).
- Ascertaining the legality and appropriateness of re-identification and repurposing of personal data collected in the provision of a network connection.
- Dealing with radically different expectations among students as to how and when data about personal activities should be made available and actionable.
- Opening debate over future increases in levels of data collection, which could make some individuals or groups identifiable if the data were combined with other sources (i.e., some courses have relatively few students).
- Engaging a range of students in thinking through longer-term issues, directions and possibilities related to the 'smart campus' and personalised learning that integrate online 'Learning Analytics' with physical presence.

Some more general issues became clearer too. As an information privacy-led principle, data protection law insists that data not be excessively collected for a particular purpose. However, in order to determine the minimum level of data needed to create a valuable service, there needed to be limited periods of research in which there may be an over-collection of data. This is particularly necessary when developing a predictive model and identifying the metrics that need to be collected and processed. More careful guidance on how this can be justified and achieved as a research process with ethical oversight is required. This in turn highlights the need to remedy the lack of formal processes for the

ethical review of University management and service operations, as distinct from ethical review procedures in research and teaching.

4.3 CitySounds: Monitoring biodiversity in an urban greenspace

Acoustic data can be a source of important information about events and the environment in modern cities. Within the context of environmental monitoring, most of the effort involving sound has been motivated by the need to monitor, and eventually control, noise pollution, as required by the European Noise Directive (END, 2002). However, it is also recognised that the urban soundscape contains a rich variety of signals that can inform us about the health and wellbeing of both humans and nature (Braubach et al., 2017; Gidlöf-Gunnarsson and Öhrström, 2007; Vianna et al., 2015).

The CitySounds project (Klein et al., 2018) installed a number of sensor kits at several locations within The Meadows: an urban public greenspace adjacent to the central University campus. Adjacent to a large area of traditional housing that now provides private rented accommodation for many students, The Meadows are constantly traversed by foot and bicycle by University students (and staff) on their way to and from the University's central campus, and are also frequently used for recreation by Edinburgh residents, including children, tennis players, joggers, and cricket players. Fun fairs, Festival events and other entertainments are frequently mounted in The Meadows as well. During the lifetime of the project (November 2017–April 2018), the acoustic monitoring devices of CitySounds regularly captured short clips of ultrasonic and audible noises of bats, birds and other wildlife, traffic, and human activity in real time. The sounds were combined with other data from the sensors, such as temperature and relative humidity. It was hoped that they could eventually be used to answer questions such as: How active is the bat population in this area? Does traffic noise change animal behaviour over the course of a day? What is the pattern of human activity during different seasons of the year?

A key partner for the project was Edinburgh Living Landscape,[11] a consortium of organisations, including the City of Edinburgh Council, that maintain a focus on biodiversity

[11] See https://edinburghlivinglandscape.org.uk/

in urban environments. The consortium's joint policy objective is the search for more efficient and reliable ways to use new and existing data to inform land management at the ecosystem-scale for the benefit of people, wildlife and the economy. Following user co-design and public engagement, the project worked closely with Friends of the Meadows and Bruntsfield Links (FOMBL)[12], an organisation of local residents that helps to protect and enhance The Meadows and organises a programme of volunteer-led biodiversity projects. In order to respond to the interests of these stakeholders, the project agreed that the audio-capture equipment would be capable of capturing sounds in both the ultrasonic range (to monitor bats) and the audible range (to monitor birds and potentially insects). However, it was clear from the outset that if audible sounds were collected by microphones, it would not be possible completely to eliminate the risk that some of the audio data would contain traces of voice from passers-by. If the content of such spoken utterances were intelligible, it might contain information that would enable the identification of specific individuals and would therefore constitute personal data. It was important that the project's use of microphones was not, and was not perceived as, an audio surveillance system aimed at gathering information about human speech, conduct and interactions. In order to allay these concerns, the project team consulted closely with the AG as well as the University's Data Protection Officer.

As a result, the project implemented measures that were designed to meet both ethical and legal requirements. These included:

- An information leaflet posted on existing glass-fronted notice boards in key locations across The Meadows; a QR code and URL on the leaflet directed people to the privacy notice on the project website.
- A detailed PIA, which was published in PDF format on the project website.
- A two-fold approach to ensure that any audio data that was shared outside the project contained no personal data:
    - Manual filtering of the audio data to select samples that contain no speech and thus require no further processing to ensure privacy.

[12] See http://www.fombl.org.uk/

    - Where manual filtering is infeasible or leads to inconclusive results, application of an algorithmic voice-scrambling process to the audio sample that renders speech unintelligible; the effectiveness of the process was assessed by an independent expert from outside the University.
- Establishment of a procedure for handling enquiries and complaints from members of the public.

In further discussion about the project's ethical aspects, the AG and others raised criticisms about the limited extent of community consultation. That is, while the project team disseminated information, and invited feedback, about the audio collection via its stakeholder partners and their networks, it was argued that more could be done to consult a broad range of members of the public who traverse or carry out activities within The Meadows. This suggestion, while well taken, raised two problems. First, when this point was raised, the period of external funding for the project had terminated and it was unclear how to resource such an engagement exercise. Second, the team lacked a principled basis for determining what would count as a representative sample of the community of users.

5 Issues arising from use cases

The three use cases presented above can be understood, to a certain extent, as characteristic of those generated by a UK research university. First, the University is a large employer and consequently has many opportunities to use IoT technology to increase operational efficiency. At the same time, the University has not so far developed an 'intelligent campus' or a culture of workplace monitoring of the kind accepted as routine in other sectors, such as road haulage or service centres, and would likely encounter vocal resistance from staff if it attempted to impose such a culture.

Second, as part of a broader trend within higher education in the UK and elsewhere, the University's relationship with students is increasingly seen as a commercial exchange: students pay significant fees to the institution and in return expect a commensurate level of 'service'. As a result, the University has become increasingly sensitive to the pressures

arising from student feedback and this in turn has led to efforts to 'improve the student experience', as exemplified by the desire to provide an information system in the Library that will allow students to manage their study time more effectively. This is not so dissimilar to the way in which transport operators provide real-time information to allow the public to plan their journeys more efficiently. Not surprisingly, the concept of a 'smart campus' (Bates and Friday, 2017; Kerr, 2017; Sari et al., 2017), driven by data from pervasive connected devices, has begun to gain momentum and has been framed as 'the intersection between Smart Homes (new experiences for Digital Natives entering higher education) and Smart Cities (new operational efficiencies to save money and improved public safety)' (Nedwich, 2018).

JISC's (2018) promotional guidance on the 'intelligent campus' identifies many significant uses of IoT that may redound to the advantage of higher education participants, whether students, academic staff, or administrative personnel. At the same time, it also identifies a number of ethical issues that need to be addressed in several areas: awareness and control of one's own data and its usage; respecting individual privacy; appropriate interpretation and decision making; and clear and transparent processes and policies (JISC, 2018, pp. 24–28). These areas principally concern the use of personal data, and in each area some sub-issues and questions are recognised that would need to be handled as part of governance strategies, instruments and organisations. These are valuable pointers, but there are further ethical issues that could too easily fall below the radar: issues about, for example, who benefits and who does not; who participates in decision-making for the deployment of intelligent devices and the data they collect; and the desirable extent and limits of surveillance. These are not fully confronted and remain to be debated as campuses migrate to becoming 'intelligent'. Moreover, the scope and specifics of necessary institutional innovation for governance of these processes need to be explored further.

Our third use case exhibits some characteristics of 'Smart City' innovation, which are often collaborations between Universities and municipal government that include monitoring of public space. As such, there is a clear imperative to identify and work with stakeholders outside the ambit of the University, including not only ordinary city residents but also community groups concerned with greenspaces and biodiversity. At the same time, of the

three examples, it is the only one that falls within a largely standard framework of academic research, governed by University ethics clearance procedures and by the ethics requirements of the external funding body.

The exposition of use cases indicates that there are many open issues regarding the ethical dimension of IoT that require thought and practical attention. There is little space here to develop a deep analysis of these issues, but they warrant some discussion if only to shape an agenda of unfinished business that is likely to confront the further development of the Initiative, of IoT more generally, and indeed of data-driven innovation.

5.1 How and when to engage 'users'

A key challenge for IoT projects in 'real' situations is how to engage users early in the development cycle; arguably, the use cases were somewhat deficient in this regard. Nevertheless, it is important not to underestimate the practical difficulties that arise in carrying out effective user engagement. This is especially acute for proofs of concept that require testing in the 'wild', or with real-life users who may not have given their consent (e.g., almost anything deployed in a public space, including facial recognition and device tracking) or on live services (e.g., electricity meters). These challenges are not unique to IoT; they plague all attempts to involve 'users' in innovation-focused projects.

As we saw in the office occupancy monitoring project (section 4.1), contacting all potential meeting-room users via email at the start of the project fails on at least two counts: (i) the information is poorly contextualised for the audience and is unlikely to be perceived as relevant or important, especially given a high volume of email communications and announcements; and (ii) until the system has been deployed, users have little or no information about the kind of interaction in which they will be involved. Similarly, attempting to communicate with users via an information notice is unlikely to anticipate the questions users ask, and is unlikely to attract feedback and discussion except perhaps when someone has extremely strong objections. Although users were given the opportunity to provide input or to ask questions via a web contact form, issues around

privacy or ethics did not surface, either for the office occupancy project or for the CitySounds project.[13]

Attempts within our three use cases to engage with users by a combination of interviews, focus groups and participant workshops were somewhat effective, but the following points are worth noting. First, face-to-face methods of communicating with users will be expensive: they require significant time for planning and execution and require skilled personnel to carry out the work and analyse the results. For short and largely experimental projects, it is often not feasible to find the time and resources to carry out these engagement processes.

Second, these methods require a time commitment from the users that they may well be unwilling to make in the absence of strong incentives. Related to this is determining what is, and gaining access to, the 'relevant' population. In the case of the office monitoring project, there was a well-defined set of users, namely the building occupants; even so, it required significant efforts to persuade even a small sample to participate in a qualitative survey. By contrast, the potential user population for CitySounds was large and poorly circumscribed, and within the scope of a five-month project it was hard to make links with the relevant communities.

Third, there is a temporal dilemma: it is typically the case that some initial prototyping by the project engineers needs to take place in order to identify what is feasible given the available hardware and software resources and the physical context within which deployment will take place. Consequently, even where a project has budgeted sufficiently for, say, engagement workshops, it may be difficult to establish the point at which sufficient progress has been made with initial prototyping to allow useful and informed participation by stakeholders, and possible implementation of their suggestions in the further design of the project.

---

[13] Given the short duration of the office occupancy pilot project, the project leaders and the AG did not have time to engage with trade-union representatives as interested and protective parties. The strategic importance of liaising with union representatives was however recognised by the Edinburgh IoT Programme Board.

5.2 Promoting ethical and responsible research

Until recently, curricula in computer science, engineering, and a range of other fields have normally included rather limited education in, or appreciation of, the ethical, social, legal, economic and other implications of technical development. However, an understanding of these implications is now being seen in a clearer light by commentators on technological and social matters, pointing to the need for awareness of the consequences of research and innovation, and for ways of acting on this awareness in the innovation process, not least in the fields of development and application involved in IoT. Communities of IoT practitioners with a focus on responsible and human-centred IoT are also emerging (ThingsCon, 2017). Legislation such as the GDPR broaches this issue by its requirement for data protection 'by design and default' and by its requirement for data protection impact assessment (DPIA). While this forms one of the bases for 'ethical' practice, it is only one element. Whether, and how far, an ethical culture of IoT development can be built into the education and training of technologists, and into their job and project specifications, is a current and future question with far-reaching implications. It also raises the challenge of who counts as the 'technologist' who might need this education, when plug-and-play, off-the-shelf IoT components might be being deployed by hobbyists, artists, biologists, retail managers or librarians.

5.3 Trust and trustworthiness in the socio-technical systems of IoT

Sometimes amplified by the media, stories about topics such as data breaches, and intrusive and unaccountable surveillance (sometimes targeted at vulnerable or disadvantaged groups) threaten to damage trust by revealing the non-trustworthiness of those who develop and deploy these technical systems. Organisations such as the University of Edinburgh worry about their 'brand' and reputation, and are careful to gain and maintain public trust in their IoT systems and services in terms of likely benefits (individual, social) and the minimisation of harms. The soundest means to this end is the demonstrated trustworthiness of innovators, companies, and researchers through robust systems of transparency and accountability (see e.g. Bihr, 2017) that can both anticipate likely trust-damaging events involving IoT and communicate credible accounts if such

events occur. Devising these systems is still in an experimental stage in many organisations, including the academic sector, both in terms of the purposes to be served by trustworthy reputations and in terms of the ways in which they can be gained, maintained, and repaired if necessary.

5.4 Designing procedures for governance, transparency and accountability

There is a legislative push in and across many countries towards establishing procedures for governance, transparency and accountability as essential elements of innovation itself (Jirotka et al., 2016; Stahl et al., 2014). Where to situate the machinery for these desirable components in companies, academia, and the public sphere, how to specify their operation, and how to ensure that they are effective, remain as unfinished business for IoT and indeed for ICT more widely. Once again, no one size will fit all, but there may be a tendency towards minimal provision of these elements unless pressure is maintained from inside and outside particular IoT projects. In addition, issues of commercial secrecy may militate against implementing these elements of innovation.

6 Tensions, conflicts and trade-offs

Some of the issues sketched above point to tensions of various kinds. Perhaps especially in the current climate of binary thinking in the media and social discourse, it has been too easy to conceptualise 'tensions' as difficult-to-resolve 'conflicts' that can only be settled through having zero-sum winners and losers, or unspecified formulas of 'trade-off' or 'balance'. Understanding whether, and which, tensions are truly conflicts, and how they can be plausibly understood and handled through creative resolution, seems to be an exploration well worth undertaking. Yet not all circles can be squared through trade-offs or balances, and 'wicked' problems remain. The following subsections highlight a number of such tensions.

6.1 Between ethics and curiosity-driven research

Ethics is often seen as cutting across demands that curiosity should not be limited by precepts and principles that do not belong in the world of science and knowledge. It is said that law is often onerous enough — although scientists and technologists have learned to live within its bounds in liberal democratic societies — but that ethics imposes an additional, often arbitrary set of constraints on innovation and the search for knowledge. Efforts to develop a novel application may founder in the face of 'ethicising' the work, particularly where resources and expertise in engaging with ethics, users and other stakeholders are not available. Against this is the argument that there are other important values or interests besides those of knowledge that should shape research and its application, and that this is what 'responsible research' requires. In addition, an ethics-aware innovation process may improve the research and its application by revealing new research questions, refining methodological choices, and suggesting a redefinition of problems and solutions.

6.2 Between different framings

Project proposals necessarily involve framing problems, opportunities and actions within the scope and knowledge of the proposers. In the field of IoT, solutions are framed in terms of particular types of technical application to solve the problems. Once a technical solution is proposed, it can be difficult to recast the problem in a way that identifies non-technical solutions, e.g., behavioural, social, cultural, or organisational. As a result, problems come to be understood as only resolvable by technology. By engaging in consultations, new entrants and non-technologists can redefine and reframe the problem and bring power relationships into clearer focus.

6.3 Between developing a technical solution and conducting research to examine the validity of the solution

In the three use cases discussed earlier, technical considerations loomed large in determining the functional scope and success criteria of the projects. Both the office monitoring and CitySounds efforts were intended, at least in part, as pilots that would allow

the University's IoT infrastructure to be explored and tested. However, this approach ran the risk of constraining too narrowly the set of stakeholders with a say in determining 'what works'. In an alternative perspective, trialling an IoT solution would not be restricted to system development but would involve research into how the solution addresses the varying needs and priorities of the stakeholders and investigate how users actually interact with the experimental system. This requires a push towards a more socially aware 'research mentality' among developers and the subsequent use of established research methodologies and research ethics procedures.

6.4 Between achieving purposes and wider, long-term, or unanticipated effects

The use cases illustrate that IoT projects are established for certain purposes. On the data protection side, the PIA or DPIA requires these to be specific but might result in ignoring information about the wider effects of data processing, or about non-data-related issues. DPIA requires an assessment of the risk to the rights and freedoms of data subjects, but this tends both to individuate the effects and to highlight definable rights and freedoms rather than wider effects (Wright and Raab, 2014). This may fail to encompass consequences that are better comprehended in social or collective terms (Cramer, 2018; Taylor, 2017) and in terms of interests that may not be codified as rights or freedoms. Moreover, long-term and unanticipated effects are likely to be left out of account, such as discriminatory effects upon certain categories of Library user as a result of the new patterns of space usage, or possible adverse effects on the texture of student life if space monitoring were to become ubiquitous across the University. It might be unreasonable or impossible to take such effects completely into account (especially when dynamic interactions between system, context and user are involved (Singh et al., 2018)), but an ethical approach might encourage such anticipatory thinking, research and debate at an early stage of planning new IoT applications, in which other purposes (e.g., exercising a duty of care towards students, saving energy, or fire safety) are part of a project brief.

6.5 Between ethics and the management of reputational risk

Tension can be seen between two stances on ethics. One is that 'doing the right thing' (or avoiding the wrong thing) prioritises the rights and needs of people as the rationale for developing ethical principles and procedures. This contrasts with a focus on the reduction of institutional risk by ensuring that ethics is integrated into the research and innovation process. The first stance would tend to place fewer restrictions on the lengths to which ethics should go, because avoiding harm to individuals, groups, and societies — and benefitting them — are vitally important. The second stance would tend to measure risks to determine their 'acceptability' to the institution (government, university, company, project, research team) and set a lower target. There may even be tension between considering institutional risk and the commercial requirement for market success. For example, a start-up company might decide that reputational risk should be subordinate to the risk of not bringing a viable product to market on time. Reconciling these two perspectives might be difficult in practice, and how the public perceives the goals of institutional ethics initiatives is an important factor in handling this issue.

6.6 Between ethics and public opinion

Normative ethics indicate what ought or ought not to be done, evaluated by criteria that have roots in philosophical reasoning, although different schools of philosophy do not necessarily point in the same direction. Ethics are, in principle, separate from the determination of what ought or ought not to be done through the gathering of public opinion, although ethics and public opinion may coincide. Ascertaining public opinion on privacy, security, surveillance and trust is notoriously difficult, and there are severe problems with survey research on these topics.[14] Moreover, survey results might give no clear guide. However, in specific contexts, such as the IoT use cases, finding out how the *relevant* public understands and feels about the benefits or harms of such data usage through public engagement exercises can to some extent provide proxies. These have some normative weight and gain valuable information and insights for IoT design and

[14] As the EU FP7 PRISMS project showed; see Friedewald (2015).

application but cannot act as a normative trump-card over ethical deliberation. Public opinion is often solicited to see what the (majority of the) relevant public is 'comfortable' with. However, ethics might well be 'uncomfortable' but necessary, based on defensible — albeit debatable — philosophical grounds. Tension between ethical schools is one thing; tension between ethics *tout court* and public opinion is another.

6.7 Between transparency/accountability and cybersecurity

Transparency and accountability are normally regarded as a 'good thing', recognised in ethics principles and procedural requirements as well as in legal requirements. They are implicated in some of the other tensions identified here. On the other hand, the security and dependability of IoT devices and processes may be compromised by the way transparency and accountability are implemented in projects. Knowing the precise location of sensing devices might facilitate tampering and other damage to IoT equipment and knowing the details of information-processing IoT systems might facilitate attacks on software or introduction of spurious data. Satisfying the requirements of both physical security and of transparency and accountability is often problematic and a 'balancing' approach might not satisfy either requirement. In any IoT systems that process personal data, ensuring robust security is crucial to the ability of the systems to comply with legal requirements for data privacy. On the other hand, if users might expect or demand that data be made available to them on grounds of utility — for example, Library users wanting to see the pattern of their own activity as collected by the monitoring system so that they can more effectively make choices in using spaces — such requests might conflict with cybersecurity requirements, and ways of reconciling these competing interests might be difficult to devise.

6.8 Between academic and external partners

The IoT Initiative, like many other R&D programmes, involves collaborations between participants situated in academic and business or public sector contexts. In any area of human activity, partnership itself gives rise to tensions, but there are well-known legal and social ways of keeping them in check and resolving disputes. The admixture of ethical

requirements, however, can create further tensions and make resolution difficult for partners who have very different expectations or 'stakes' in the process and outcomes of the IoT partnerships, perhaps institutionally and culturally shaped (e.g., different understandings of 'success' in academia and business). The likelihood of these tensions arising is increased when universities are under pressure to measure their success in terms of attracting funding from large corporate partners. The situation of ethics within the partnership, within the different criteria for 'success', and within different degrees of exposure to public appraisal, trust or scepticism, may generate tensions as well as place the particular ethical regime and its governance under strain if, for example, the principles are not viewed in the same way by all.

7 Principles and procedures

With the perception that law alone is inadequate for safeguarding human rights and values, including privacy and data protection, there has been a 'turn' to principles in the literature and practices of ICT and related developments such as AI and IoT. The grounds for this perception are debatable, but there is a plethora of 'ethics' guidelines, principles, procedures, etc. on which to draw for IoT purposes (Raab, 2020).[15] Some of these normative frameworks are highly elaborate, blurring the distinction between overarching principles and practical procedures. Codes of practice or conduct exist for many academic disciplines, drawn up by professional associations and others. There are also laws that pertain to such research, overlapping with some ethical principles and codes, and resting on rights, perhaps especially privacy. The Draft Ethics Guidelines for Trustworthy AI (AI HLEG, 2018) by the European Commission's High-Level Expert Group on Artificial Intelligence lists five principles: beneficence, non-maleficence, autonomy, justice and explicability. These, or variations on them, are found in many other lists. Clarke's (2019) more elaborate inventory identifies ten general and fifty specific principles for responsible

[15] For discussions of this plethora in the related field of artificial intelligence (AI), see Jobin et al. (2019) and Morley et al. (2020)

AI, although many of these are procedural derivatives. It may be preferable to distil the principles themselves down to a very few, perhaps five to ten.

The AG's work on principles and procedures involved a review of existing frameworks and lists as well as internal discussion and consultation, with an eye towards encompassing research and practical uses of the IoT Service. The approach was iterative and much of the drafting of the principles was interleaved with learning about, and providing input to, the use cases described earlier. Uncertainty exists about likely future use cases to which ethical approaches would apply and about the practical applicability of even the most unexceptionable principles. This process of deliberation has resulted in a working inventory of nine principles and seven procedures that should apply to specific projects within the Initiative (Raab et al., 2018). It was emphasised that, beyond compliance with data protection law, project leaders should aim to determine whether, and how, legal and ethical principles are relevant to a project's specific circumstances, how to take them into account, and how to implement them. This list of principles resonates with those found elsewhere, but also has regard to non-human and environmental values owing to the heterogeneity of IoT applications. The principles apply to the conduct of an IoT project, including the processing of data, and to the use of the research and the practical outcomes of the project. It was recognised that principles are more likely to gain traction with project leaders and less likely to be seen as obstacles to innovation rather than as contributory elements if they are complemented by guidelines, information, advice, resources and practical procedures.

Principles and procedures that are 'portable' across fields of application are valuable: these ideas can be easily communicated and used to raise broad awareness. But principles and procedures are not sufficient, since community support and the creation of discourses and tools are required to enable people to use them.[16] It is obvious that a whole range of supportive governance mechanisms, resources, and infrastructural activity also needs to be put in place to promote the implementation of procedures and principles. These include

[16] In a similar vein, Mulgan (2019) has emphasised the importance of supplementing ethical principles with contextual application and reasoning.

giving support to ethics officers; providing training and advice; providing resources to develop a community of practice; and critical evaluation at the IoT service level as a continuing participatory and reflective process. This is work that the AG aimed to undertake for the IoT Programme, and much of it is congruent with the likely requirements for ethical frameworks and principles pertaining to broader data-driven innovation pursuits, including AI, within the University's Data-Driven Innovation programme.[17]

8 Conclusion

In the context of research, education, and organisational management, IoT presents new challenges to existing practices of ethics. Some of these challenges pertain to the inquisitive nature of research projects while others have to do with the institutional constraints and advantages in the settings in which IoT projects and implementation take place. In the case of the Initiative, IoT emerged as an infrastructural addition aimed at solving problems and at supporting research and innovation. Because of this, the activity around IoT, in terms of research and practical use 'in the wild', cuts across many disciplinary and institutional boundaries, which often contain different expectations about ethical considerations (e.g., medicine v. computer science, formal v. informal ethical evaluation). Any individual project may suffer from gaps in the quantitative, qualitative and conceptual expertise that may be necessary for framing and evaluation.

We have provided evidence for such issues by describing three use cases that make use of IoT in different fashions, serve different publics and are variously managed from an institutional point of view. The work of the AG contributed to a continuing and wide-ranging reflective debate on the implementation of the projects and had a twofold immediate impact: it consolidated and extended the role of ethics and accountability in the shaping of the IoT Initiative's practices and — perhaps with less certainty — it incorporated IoT as a matter of concern for ethics officers across the University. An

[17] See https://ddi.ac.uk/

outcome of this reflective process was an amendable set of principles and procedures that serves as an applicable tool.

Additional lessons emerged from the attempt to bring ethics into the processes of University IoT development. One is that there are unlikely to be clear temporal and spatial 'beginnings' of the University's IoT applications into which, or alongside which, ethical or 'responsible innovation' principles and guidance might be located. The formation of IoT projects, practices and policies take place at various locations in the institution and on various agendas. The role of ethics and of an ethics machinery such as the AG cannot be envisaged as a command-and-control, top-down attempt to overtake the development processes for these innovations. It is, rather, a contributory element that has to develop its influence through achievements in providing what the University's community of IoT providers and recipients perceives as useful, either in the reputation-preserving coinage it can produce, or in the deeper normative value it can provide.

A second lesson concerns legitimacy and effectiveness. The cogency of such an ethical component to IoT depends in considerable part on the legitimacy and material resources that its proponents can gather within an institution in which IoT is only one domain of research and innovation. The traction that better ethics and governance can gain within IoT requires borrowing legitimacy (e.g., from the data protection requirements that overlap with ethics) and securing material resources to engage in enquiries, acquire research assistance, and spend academic time in ways that could ultimately provide evidence of effectiveness. But IoT is only one of a broader, more comprehensive and better-resourced constellation of technological ambitions and visions within the University. These latter plans are themselves facing similar questions about ethical and responsible innovation in a context that is composed of academic and non-academic partners, and with considerable interest shown by governments. Within this context, the IoT Initiative's ethical work could serve as a pilot for wider adoption. If so, such recognition would lend legitimacy to the AG's efforts to influence the IoT domain, but evidence of successful influence in IoT — as distinct from 'busyness' — is difficult to demonstrate at this early stage. There is thus an element of bootstrapping in the search for legitimacy and effectiveness.

The context of the University's IoT Initiative will differ in many respects from the realm of industrial, municipal and commercial IoT products and services. One aspect is the current application domain of the IoT infrastructure, which in this case is mainly oriented to sensing and monitoring. Thus, it covers only a subset of the wider scope of IoT and perforce only a fraction of the universe that is loosely labelled 'data-driven innovation'. Another differentiating aspect is the non-commercial, research-oriented and 'public-good' character of the infrastructure. Likewise, as we have seen, our ethical framework is designed for University practitioners and academic research projects, while 'intelligent campus' and Smart City initiatives are often shaped by goals, methods and timelines that are more aligned with industry-oriented practice. Of course, there are also public sector IoT initiatives, perhaps especially at the municipal level, in which the need for ethical legitimacy and the development of ethical frameworks is being realised by a variety of actors. From the perspective of comparable domains of IoT innovations in the public and private sector, efforts to develop ethical principles and procedures along the lines presented in this article can offer a useful counterpoint.

Bibliography

AI HLEG. (2018). *Draft Ethics Guidelines for Trustworthy AI*. EC Directorate-General for Communication. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57112

Baldini, G., Severi, S., and Hennebert, C. (2015). *IoT Governance, Privacy and Security Issues* [IERC Position Paper]. European Communities. http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

Bates, O., and Friday, A. (2017). Beyond Data in the Smart City: Repurposing Existing Campus IoT. *IEEE Pervasive Computing*, *16*(02), 54–60. https://doi.org/10.1109/MPRV.2017.30

Bauer, M. (Ed.). (1995). *Resistance to New Technology*. Cambridge University Press. https://doi.org/10.1017/CBO9780511563706

Bihr, P. (2017). *A Trustmark for IoT: Building consumer trust in the Internet of Things by empowering users to make smarter choices* [ThingsCon Report]. ThingsCon. https://thingscon.org/publications/report-a-trustmark-for-iot/

Braubach, M., Egorov, A., Mudu, P., Wolf, T., Thompson, C. W., and Martuzzi, M. (2017). Effects of Urban Green Space on Environmental Health, Equity and Resilience. In *Nature-Based Solutions to Climate Change Adaptation in Urban Areas* (pp. 187–205). Springer, Cham. https://doi.org/10.1007/978-3-319-56091-5_11

Clarke, R. (2019, February 20). *Principles for Responsible AI*. http://www.rogerclarke.com/EC/PRAI.html

Clay, J. (2017, July 13). There's no room! *Intelligent Campus*. https://intelligentcampus.jiscinvolve.org/wp/2017/07/13/theres-no-room/

Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Amar, Y., Mortier, R., Li, Q., Moore, J., Wang, L., Yadav, P., Zhao, J., Brown, A., Urquhart, L., and McAuley, D. (2018). Building accountability into the Internet of Things: The IoT Databox model. *Journal of Reliable Intelligent Environments*, *4*(1), 39–55. https://doi.org/10.1007/s40860-018-0054-5

Cramer, B. W. (2018). A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance. *Journal of Information Policy*, *8*, 5–33. JSTOR. https://doi.org/10.5325/jinfopoli.8.2018.0005

END. (2002). Environmental Noise Directive (END). 2002/49/EC of the European parliament and the Council of 25 June 2002 relating to the assessment and management of environmental noise. *Official Journal of the European Communities*, *L 189*(12). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0049

Friedewald, M. (2015, July 31). *PRISMS: Privacy and Security Mirrors*. http://friedewald.website/prisms-privacy-and-security-mirrors/

GDPR (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 1 (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Gidlöf-Gunnarsson, A., and Öhrström, E. (2007). Noise and well-being in urban residential environments: The potential role of perceived availability to nearby green areas. *Landscape and Urban Planning*, *83*(2), 115–126. https://doi.org/10.1016/j.landurbplan.2007.03.003

Hijmans, H., and Raab, C. (2018). Ethical Dimensions of the GDPR. In M. Cole and F. Boehm (Eds.), *Commentary on the General Data Protection Regulation*. Edward Elgar. https://papers.ssrn.com/abstract=3222677

Hyysalo, V., and Hyysalo, S. (2018). The Mundane and Strategic Work in Collaborative Design. *Design Issues*, *34*(3), 42–58. https://doi.org/10.1162/desi_a_00496

ICO. (2019, January 31). *Accountability and governance*. https://icoumbraco.azurewebsites.net/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Jameson, S., Richter, C., and Taylor, L. (2019). People's strategies for perceived surveillance in Amsterdam Smart City. *Urban Geography*, *40*(10), 1467–1484. https://doi.org/10.1080/02723638.2019.1614369

Jiang, X., and Landay, J. A. (2002). Modeling privacy control in context-aware systems. *IEEE Pervasive Computing*, *1*(3), 59–63.

Jirotka, M., Grimpe, B., Stahl, B., Eden, G., and Hartswood, M. (2016). Responsible Research and Innovation in the Digital Age. *Communications of the ACM*. https://ora.ox.ac.uk/objects/uuid:b8d67d60-6115-4ed0-b8d8-15d5d501b1f5

JISC. (2018). *Guide to the intelligent campus: Using data to make smarter use of your university or college estate*. https://repository.jisc.ac.uk/6882/1/Intelligent_Campus_Guide.pdf

Jobin, A., Ienca, M., and Vayena, E. (2019). Artificial Intelligence: The global landscape of ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kerr, R. (2017, November 15). *How the Internet of Things will help enable the 'Smart Campus'*. CENSIS. https://censis.org.uk/2017/11/15/how-the-internet-of-things-will-help-enable-the-smart-campus/

Klein, E., Chapple, S., Fainberg, J., Magill, C., Parker, M., Raab, C., and Silvertown, J. (2018). Capturing the Sounds of an Urban Greenspace. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XLII-4-W11*, 19–26. https://doi.org/10.5194/isprs-archives-XLII-4-W11-19-2018

LoRa Alliance. (2019, January 22). *LoRa Alliance Passes 100 LoRaWAN™ Network Operator Milestone with Coverage in 100 Countries*. LoRa Alliance. https://lora-alliance.org/in-the-news/lora-alliance-passes-100-lorawantm-network-operator-milestone-coverage-100-countries

MacKenzie, D., and Wajcman, J. (Eds.). (1985). *The Social Shaping of Technology* (Vol. 10). Open University Press. https://doi.org/10.1177/016224398501000421

Magill, C., Klein, E., and Chapple, S. (2018, March 28). I am not a number: Towards participatory IoT monitoring in the workplace. *Living in the Internet of Things: Cybersecurity of the IoT*. Living in the Internet of Things: Cybersecurity of the IoT, London, UK. https://doi.org/10.1049/cp.2018.0021

Martin, K. (2018). Ethical Implications and Accountability of Algorithms. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-018-3921-3

Marx, G. T. (1998). Ethics for the New Surveillance. *The Information Society*, *14*(3), 171–185. https://doi.org/10.1080/019722498128809

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., and Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, *3*(2), 2053951716679679. https://doi.org/10.1177/2053951716679679

Moor, J. H. (1985). What is Computer Ethics? *Metaphilosophy*, *16*(4), 266–275. https://doi.org/10.1111/j.1467-9973.1985.tb00173.x

Morley, J., Machado, C. C. V., Burr, C., Cowls, J., Joshi, I., Taddeo, M., and Floridi, L. (2020). The ethics of AI in health care: A mapping review. *Social Science & Medicine (1982)*, *260*, 113172. https://doi.org/10.1016/j.socscimed.2020.113172

Mulgan, G. (2019, September 16). AI Ethics and the Limits of Code(s). *Nesta*. https://www.nesta.org.uk/blog/ai-ethics-and-limits-codes/

Nedwich, R. (2018, February). *Smart Campus—Education for Digital Natives*. Dotmagazine. https://www.dotmagazine.online/new-work-and-digital-education/ICT4D/smart-campus-merging-smart-city-and-smart-home-in-education-for-digital-natives

ORBIT-RRI. (2018). *ORBIT | Responsible Research and Innovation in UK ICT*. Orbit. https://www.orbit-rri.org/

Raab, C. (2012). Regulating Surveillance: The Importance of Principles. In K. Ball, K. Haggerty, and D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 377–385). Routledge.

Raab, C. (2017). Information Privacy: Ethics and Accountability. In C. Brand, J. Heesen, B. Kröber, U. Müller, and T. Potthast (Eds.), *Ethik in den Kulturen—Kulturen in der Ethik*. Narr Francke Attempto.

Raab, C. (2020). Information privacy, impact assessment, and the place of ethics. *Computer Law & Security Review*, *37*, 105404. https://doi.org/10.1016/j.clsr.2020.105404

Raab, C., Stewart, J., Domínguez, A., Klein, E., and Chapple, S. (2018). *Principles and Procedures for Ethical IoT: University of Edinburgh IoT Initiative*. University of Edinburgh. http://iot.ed.ac.uk/files/2020/09/IoT-Ethical-Principles-v1.3.pdf

Santa Clara University. (2015, August 1). *A Framework for Ethical Decision Making*. https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making/

Sari, M. W., Ciptadi, P. W., and Hardyanto, R. H. (2017). Study of Smart Campus Development Using Internet of Things Technology. *IOP Conference Series: Materials Science and Engineering*, *190*, 012032. https://doi.org/10.1088/1757-899X/190/1/012032

Singh, J., Millard, C., Reed, C., Cobbe, J., and Crowcroft, J. (2018). Accountability in the IoT: Systems, Law, and Ways Forward. *Computer*, *51*(7), 54–65. https://doi.org/10.1109/MC.2018.3011052

Stahl, B. C., Eden, G., Jirotka, M., and Coeckelbergh, M. (2014). From Computer Ethics to Responsible Research and Innovation in ICT: The transition of reference discourses informing ethics–related research in information systems. *Information and Management*. https://ora.ox.ac.uk/objects/uuid:22b55c24-102d-48a1-87b8-d9e8561e131e

Steen, M. (2011). Tensions in human-centred design. *CoDesign*, *7*(1), 45–60. https://doi.org/10.1080/15710882.2011.563314

Stewart, J., and Williams, R. (2005). The wrong trousers? Beyond the design fallacy: Social learning and the user. In D. Howcroft and E. M. Trauth (Eds.), *Handbook of Critical Information Systems Research*. https://www.elgaronline.com/view/9781843764786.xml

Taylor, L. (2017). Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. In L. Taylor, L. Floridi, and B. van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies* (pp. 13–36). Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_2

ThingsCon. (2017). *The State of Responsible IoT* [ThingsCon Report]. ThingsCon. https://thingscon.org/publications/thingscon-report-the-state-of-responsible-iot-2017/

Urquhart, L. (2017). Ethical Dimensions of User Centric Regulation. *ORBIT Journal*, *1*(1), 17–17. https://doi.org/10.29297/orbit.v1i1.14

Urquhart, L., Lodge, T., and Crabtree, A. (2018). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, *26*(4), eay015. https://doi.org/10.1093/ijlit/eay015

van Dijk, N., Tanas, A., Rommetveit, K., and Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. *International Review of Law, Computers & Technology*, *32*(2–3), 230–256. https://doi.org/10.1080/13600869.2018.1457002

Vianna, K. M. de P., Cardoso, M. R. A., and Rodrigues, R. M. C. (2015). Noise pollution and annoyance: An urban soundscapes study. *Noise and Health*, *17*(76), 125. https://doi.org/10.4103/1463-1741.155833

Wajcman, J. (2010). Feminist theories of technology. *Cambridge Journal of Economics*, *34*(1), 143–152. https://doi.org/10.1093/cje/ben057

Weiser, M. (1999). The Computer for the 21st Century. *SIGMOBILE Mob. Comput. Commun. Rev.*, *3*(3), 3–11. https://doi.org/10.1145/329124.329126

Wiener, N. (1954). *The Human Use of Human Beings: Cybernetics and Society*. Eyre and Spottiswoode.

Williams, R., Stewart, J., and Slack, R. (2005). *Social learning in technological innovation: Experimenting with information and communication technologies*. Edward Elgar Publishing.

Wright, D., and Raab, C. (2014). Privacy Principles, Risks and Harms. *Int. Rev. Law Comput. Technol.*, *28*(3), 277–298. https://doi.org/10.1080/13600869.2014.913874